

Homework 1

Due: October 9, 2023

Points: 100

1. (25 points) Companies usually restrict the use of electronic mail to company business but do allow minimal use for personal reasons.
 - (a) How might a company detect excessive personal use of electronic mail, other than by reading it? (*Hint:* Think about the personal use of a company telephone.)
 - (b) Intuitively, it seems reasonable to ban *all* personal use of electronic mail on company computers. Explain why most companies do not do this.
2. (25 points) A company publishes the design of its security software product in a manual that accompanies the executable software.
 - (a) In what ways does this satisfy the principle of open design? In what ways does it not?
 - (b) Given that the design is known, what advantages does keeping the source code unavailable give the company and those who purchase the software? What disadvantages does it cause?
3. (30 points) Given the security levels TOP SECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED (ordered from highest to lowest), and the categories A, B, and C, specify what type of access (read, write, both, or neither) is allowed in each of the following situations. Assume that discretionary access controls allow anyone access unless otherwise specified.
 - (a) Paul, cleared for (SECRET, { B, C }), wants to access a document classified (TOP SECRET, { A, C }).
 - (b) Anna, cleared for (CONFIDENTIAL, { B }), wants to access a document classified (CONFIDENTIAL, { C }).
 - (c) Jesse, cleared for (CONFIDENTIAL, { C }), wants to access a document classified (SECRET, { C }).
 - (d) Sammi, cleared for (CONFIDENTIAL, { A }), wants to access a document classified (TOP SECRET, { A, C }).
 - (e) Robin, who has no clearances (and so works at the UNCLASSIFIED level), wants to access a document classified (SECRET, { A }).
4. (20 points) Classify each of the following as an example of a mandatory, discretionary, or originator controlled policy, or a combination thereof. Justify your answers.
 - (a) The file access control mechanisms of the UNIX operating system
 - (b) A system in which no memorandum can be distributed without the creator's consent
 - (c) A military facility in which only generals can enter a particular room
 - (d) A university registrar's office, in which a faculty member can see the grades of a particular student provided that the student has given written permission for the faculty member to see them.